

# How to configure Libraesva ESG for Microsoft 365 (a.k.a Office365)

This article addresses configuring Microsoft 365 with Libraesva ESG as your inbound and/or outbound mail gateway.

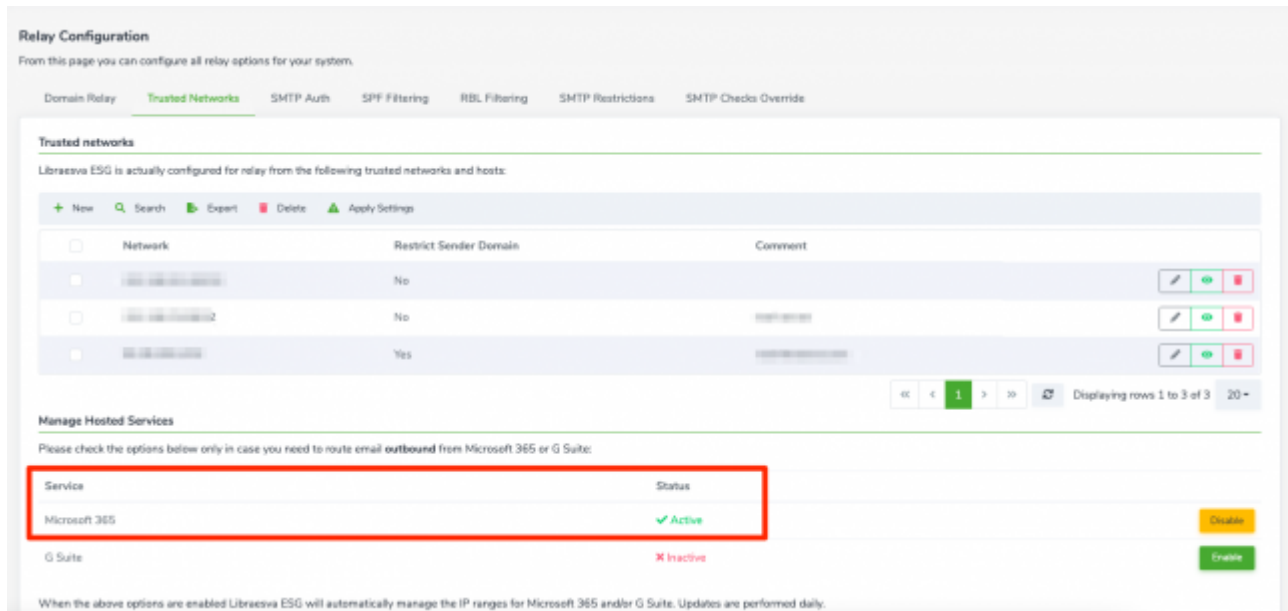
You can specify the appliance as an inbound mail gateway through which all incoming mail for your domain passes before reaching your Microsoft 365 account. Libraesva ESG filters out spam and viruses, and then passes the mail on to the Microsoft 365 mail servers. Use the Inbound Configuration instructions below to configure.

You can likewise specify Libraesva ESG as the outbound mail gateway through which all mail is sent from your domain via your Microsoft 365 account to the recipient.

As the outbound gateway, Libraesva ESG processes the mail by filtering out spam and viruses and applying any outbound policies (blocking, encrypting, etc.) before final delivery. By using the configuration described in Outbound Configuration below, you instruct the Microsoft 365 mail servers to pass all outgoing mail from your domain to the appliance.

## Preliminary Steps

- You need to have a Libraesva for Microsoft 365 valid license or an ISP license one.
- If you want to enable outbound mail flow, too, enable 365 trust by going on your **Libraesva ESG Appliance** and select Menù *System >Mail Transport >Relay Configuration >Trusted Networks* and select the option **Trust Microsoft Office 365**



# Inbound Configuration

- Log into the Microsoft 365 Portal with an admin account.
- On the left menu select **Show all** option.
- Navigate then to **Settings > Domains**.
- Select your domain from the domain list and click on it.
- Move to DNS records and spot your MX record.
- Your MX record should be something like **yourdomain-com.mail.protection.outlook.com**, your destination mail server.
- Log into the Librasva ESG web interface and go to the **System > Mail Transport > Relay Configuration > Domain Relay** menu.
- Add (or Edit if already present) the **your-domain.tld** and set the **Mail Server** field

Add record

Add a Relay Domain

Domain:
Accepted: 'domain.com' or '.domain.com' or 'user@domain.com'.

Mail Server:
Destination Mailserver IP Address or FQDN or domain

Port:
Destination Mailserver Port (Default:25)

Use MX:
Use MX resolution for final destination.

Recipient Verification:
Select recipient verification policy.

Dynamic Verification Server:
-

Dynamic Verification Port:
-

Antispoofing:
Select antispooing verification policy.

TLS Certificate:

Tag:
Enter a tag, to group items and quick search.

The Mail Server address indicates where the Libraesva ESG should direct inbound mail from the Internet (to your Microsoft 365 Exchange server).

## Recipient Verification

- **Preferred method (from version 4.6):** Configure the connector
- **Recipient Verification, alternative method:**

Alternately in Microsoft 365 you can enable the Directory Based Edge Blocking (DBEB) feature, which is similar to the Valid Recipient list in Libraesva ESG, and then enable Dynamic Verification in Libraesva ESG. Instructions can be found [here](#):

Directory Based Edge Blocking (DBEB) feature from Microsoft 365

However, if you have your own external AD/LDAP you can integrate this with Libraesva ESG to do recipient verification, streaming and authentication of user credentials.

Another solution is to set your domain on Microsoft 365 as Authoritative and always set Libraesva ESG recipient verification to Dynamic.

In addition Microsoft 365 does provide a public POP3 service which you may be able to use for authentication of users accessing the Libraesva ESG WebUI. To use these services, please contact Microsoft for details.

## Domain Antispoofing

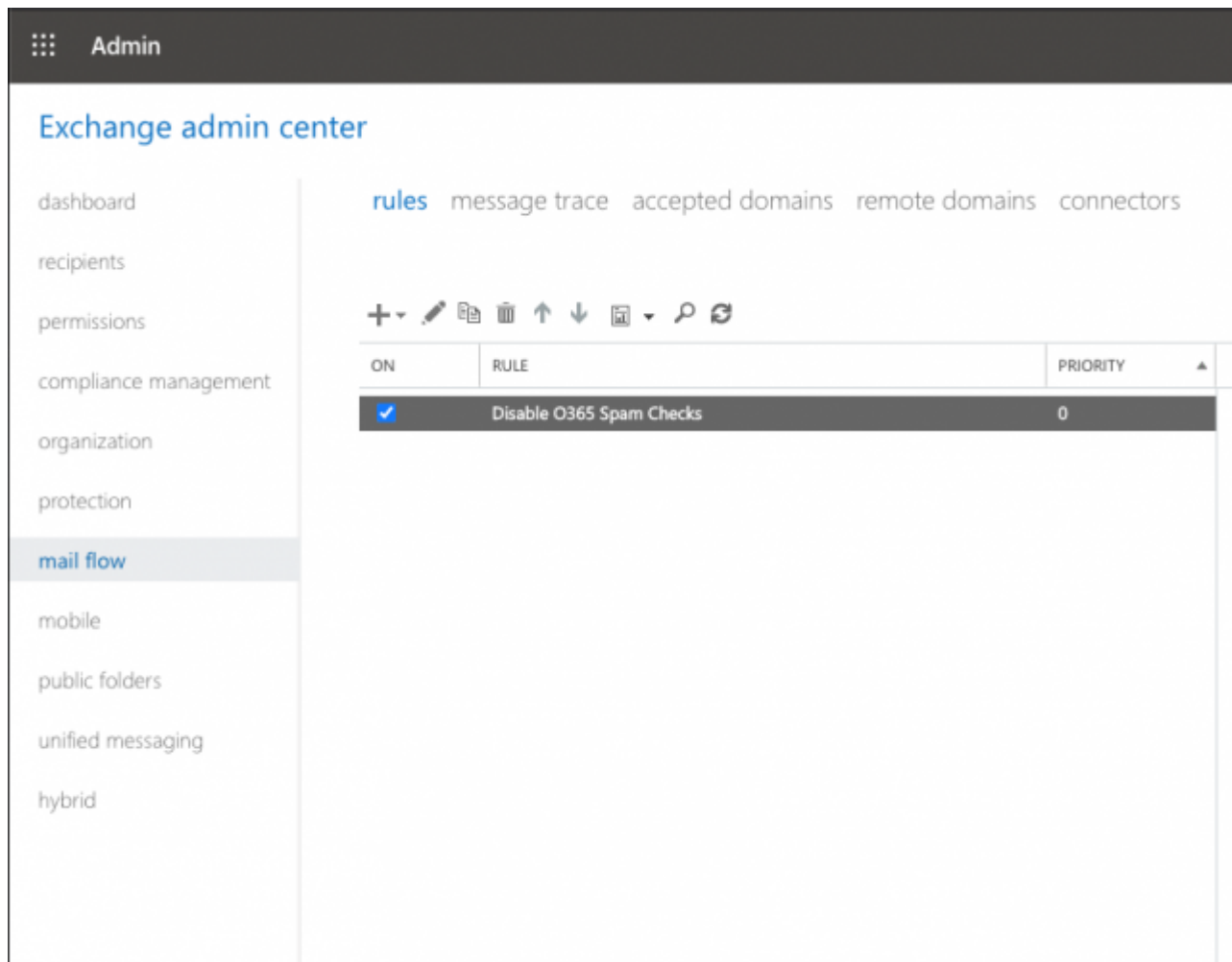
Leave Domain Antispoofing setting **Standard (SPF)** unless you are sure that no one else is sending email with your domain as envelope sender.

## Disable Microsoft 365 Spam Checks

Disabling 365 spam checks is not mandatory. We advice to disable spam checks on email delivered by Libraesva ESG in order to avoid false positives.

- In the Microsoft 365 Portal, to **disable internal spam checks** for the email analyzed by Libraesva ESG, create a **Transport Rule**:

- 1) Click on **Admin Centers** and select **Exchange** from the drop-down in the left panel.
- 2) On the left side then click **Mail Flow** link.
- 3) Under **Rules**, click the [+] button and select **Create New Rule**.



4) Give it a Name

5) Look down at the bottom and click **More options...**

6) Under the **Apply this rule if...** drop-down, select **The sender... -> IP address is in any of these ranges or exactly matches.**

7) In the pop-up titled IP address ranges, input the **Libraesva ESG IP address**

8) Click **[+]** and then click **OK**.


9) Under the **\*Do the following...** section, select **Modify the message properties...** -> **Set the spam confidence level (SCL)**, and under **Specify SCL**, select **Bypass spam filtering** via the drop-down.

10) Click **OK**, and then click **Save** to save the new transport rule.

- Do the same under the **Connection Filtering** section (<https://security.microsoft.com/antispam>).

ⓘ Please go to the quarantine policy page to configure end-user spam notification as we will remove the configuration from the Anti-spam policy by December 2021. [Learn more about quarantine policy](#)  
 Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and outbound spam filtering. [Learn more](#)

+ Create policy ▾ Refresh

Name	Status	Priority
Anti-spam inbound policy (Default)	● Always on	Lowest
Connection filter policy (Default) 	● Always on	Lowest
Anti-spam outbound policy (Default)	● Always on	Lowest

- 1) Click on **Connection Filter Policy**
- 2) Click the **Edit connection filter policy** link at the bottom of the popup
- 3) Add IP into “Always allow messages from the following IP addresses or address range” section
- 4) Click on **Save** button on the bottom of the popup

## Configure an Inbound Connector

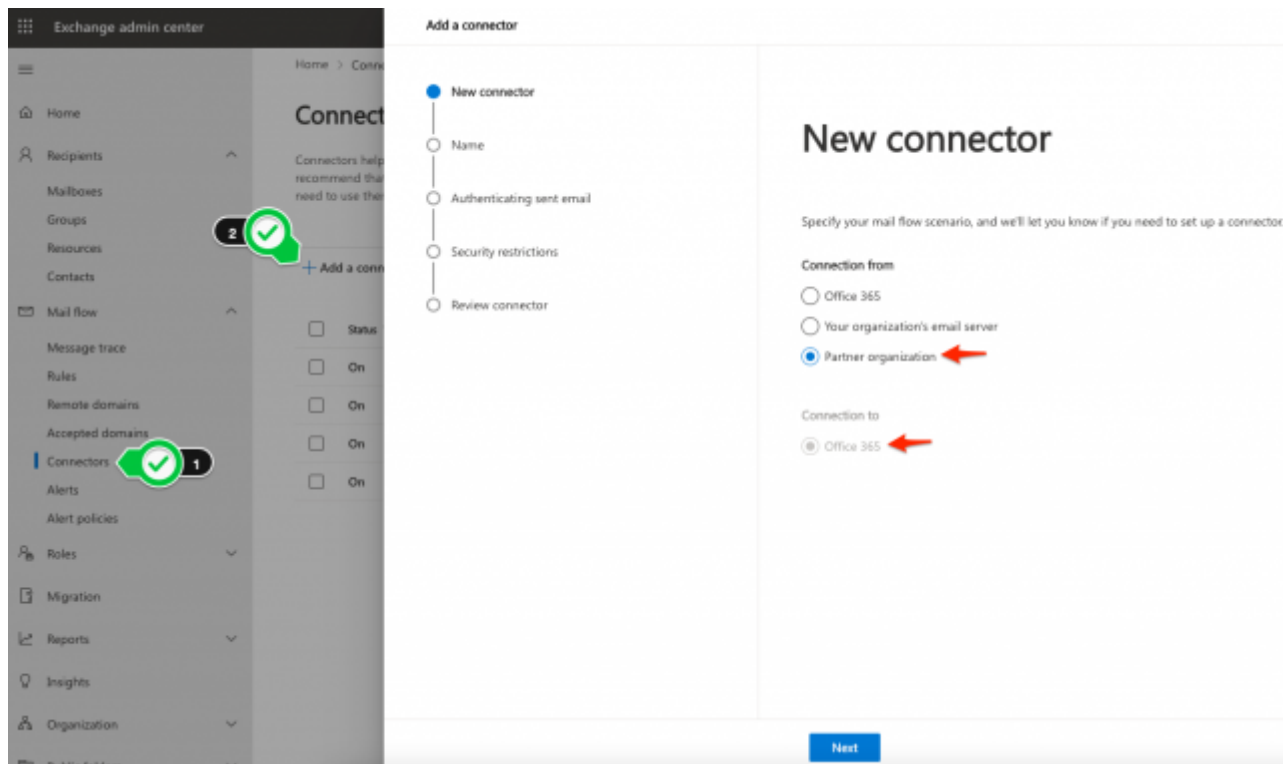
The inbound connector can be done in two ways: allowing inbound only from ESG (the right choice for production system) or allowing inbound also from other sources (suggested only when testing).

You only need one of the following connectors.

### Option 1: Lockdown the inbound mail flow to Libraesva ESG

In the Exchange Admin Center, to configure O365 to **accept email only from Libraesva ESG, reject email sent directly to Microsoft 365 and avoid Rate Limiting**, create an **Inbound Connector**:

- 1) On the left side client **Mail Flow** and select **Connectors** on the top right
- 2) Under **Connectors**, click the [+] button.
- 3) From: **Partner Organization** – To: **Office 365**



- 4) Click **Next**.
- 5) Give it a name and click **Next**
- 6) Select **Use the sender's domain**
- 7) Specify one **Sender domain** with \* (asterisk)

## Authenticating sent email

How do you want Office 365 to identify your partner organization?

Office 365 will only accept messages through this connector if your partner organization can be identified through one of the following two ways.

- ☒ By verifying that the sender domain matches one of the following domains
- 
- ☐ By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization

- 8) Click Next
- 9) Select the option **Reject email messages if they aren't sent from within this IP address range**

10) Enter the **IP Address(es)** of your Libraesva ESG appliance(s)

×**WARNING:** Steps 9 and 10 should be done after you changed the MX records. You can skip these two steps on the first setup and then come back when you received the first few messages through Libraesva ESG.

## Security restrictions

What security restrictions do you want to apply?

☒ Reject email messages if they aren't sent over TLS

☐ And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or \*.contoso.com



Step 9-10

☒ Reject email messages if they aren't sent from within this IP address range

Example: 10.5.3.2 or 10.3.1.5/24



11) Click **Next**

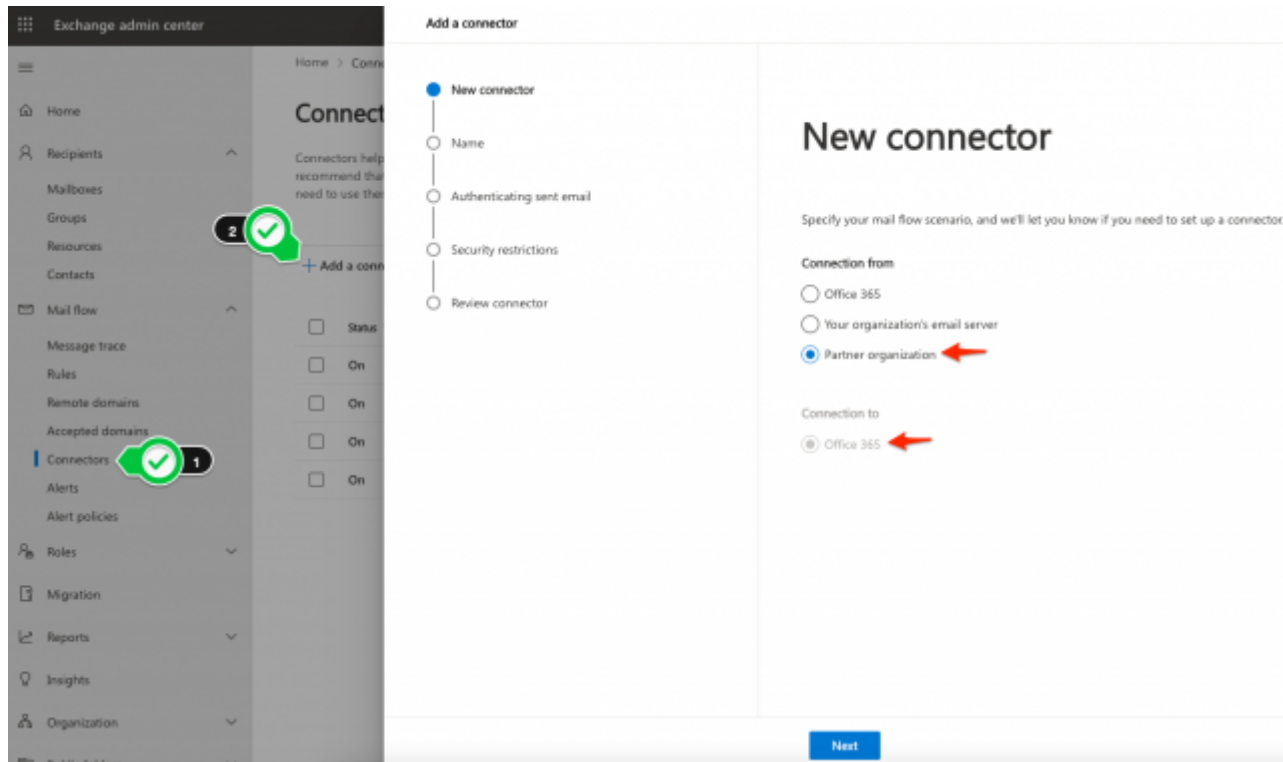
12) Review and **Create connector**

### Option 2: Accept email from any source

In the Exchange Admin Center, to configure O365 to **accept email from Libraesva ESG** and **avoid Rate Limiting**, create an **Inbound Connector**:

- 1) On the left side client **Mail Flow** and select **Connectors** on the top right
- 2) Under **Connectors**, click the [+] button.
- 3) From: **Partner Organization** – To: **Office 365**





- 4) Click **Next**.
- 5) Give it a name and click **Next**
- 6) Select **Use the sender's IP address**
- 7) Specify the **IP address(es)** of your Libraesva ESG appliance(s)

## Authenticating sent email

How do you want Office 365 to identify your partner organization?

Office 365 will only accept messages through this connector if your partner organization can be identified through one of the following two ways.

- ☐ By verifying that the sender domain matches one of the following domains
- ☒ By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization

IP

- 8) Click Next
- 9) Select the option **Reject email messages if they aren't sent over TLS** if you want for force Microsoft 365 to accept email from Libraesva ESG **only** with a TLS connection

10) Click **Next**

11) Review and **Create connector**

×**NOTE:** This is the official Microsoft documentation about adding a new receive connector in Microsoft 365.

## Modifying Your MX Record

To direct your email traffic to Libraesva ESG you need to update your domain's "MX records". The MX records are stored at your domain host and will direct your email to your mail servers. It's like registering your new address with the post Microsoft so that your mail gets delivered.

The MX record should be updated to point to your Libraesva ESG appliance.

Further information are available [here](#).

---

## Outbound Configuration

×**NOTE:** each time you add a new rule or connector, Microsoft will take till an hour to propagate over all nodes new settings.

### SPF Record

Before going through the configuration steps below please **Update the SPF Record for your domain(s)!**

Your organization should already have a SPF record for the domain(s) registered with Microsoft 365. When implementing Libraesva ESG with Microsoft 365, this record must be updated in the DNS zone for the relevant domain to include the following:

**Add: include:spf.esvacloud.com (if Libraesva ESG is deployed in our cloud)**

**Add: include:<customer-spf-record> or a:<ESG-HOSTNAME> or ip4:<ESG-IP-Address> (if Libraesva ESG is deployed in customer's datacenter)**

in both cases **include:spf.protection.outlook.com** must be present

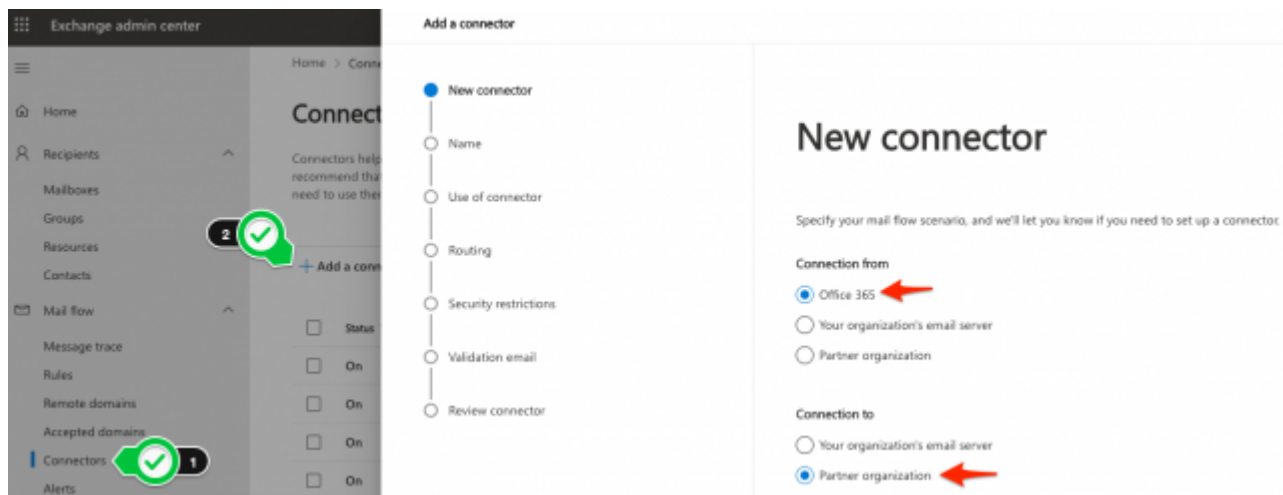
Example:

```
v=spf1 mx include:spf.proteccion.outlook.com include:spf.esvacloud.com -all
```

# Outbound Connector

To configure the outbound mail flow from Microsoft 365 to Libraesva ESG proceed as follows:

- Log into the Microsoft 365 Portal (<https://www.office.com>) .
- Click on **Admin** and select **Exchange** from the drop-down in the left panel (by clicking on Show all).
- Select **mail flow** from the left link navigation bar.
- Select the **connectors** link at the top.
- Create a new connector
- In the **From** section select Microsoft 365, and in the **To** section select Partner Organization. Click **Next**.



- Give the new connector a **Name** (for example: *Microsoft 365 to Libraesva ESG*), optional **Description**, and decide if the connector should be enabled once it has been saved using the **Turn it on** checkbox. Click **Next**.
  - Change selection on first bullet **Only when I have a transport rule....** and click on next.
  - Select the **Route email through these smart hosts** option, and click the plus icon to add the ip address or FQDN of your Libraesva ESG Appliance. Click **Save**, followed by **Next**.
- In a cluster environment be sure to add both nodes IPs.

#### Add a connector

- ☒ New connector
- ☒ Name
- ☒ Use of connector
- ☒ **Routing**
- ☐ Security restrictions
- ☐ Validation email
- ☐ Review connector

## Routing

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

☐ Use the MX record associated with the partner's domain

☒ Route email through these smart hosts

Example: myhost.contoso.com or 192.168.3.2



- Leave the default **Always use Transport Layer Security (TLS) to secure the connection (recommended)** and **Any digital certificate, including self-signed certificates** (unless you own a trusted one) set and click **Next**.

## Security restrictions

How should Office 365 connect to your partner organization's email server?

☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

☒ Any digital certificate, including self-signed certificates



☐ Issued by a trusted certificate authority (CA)

☐ And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or \*.contoso.com

- Verify your settings and click **Next**.
- **Validate** the connector by adding an external mail address (not managed by you) and click **Save**.

# Transport Rule

Now we need to create the transport rule that will be linked to the newly created connector:

- Select the **rules** link at the top.
- Create a new rule giving the name "Route messages to Libraesva ESG"
- Remember to click on **More options** link once pop-up rule opens.
- Apply this rule if -> the sender -> is external/internal -> inside the organization.
- Do the following -> Redirect the message to... -> the following connector -> Select the Libraesva ESG Outbound created before.

new rule

Name:

Route message to ESG

\*Apply this rule if...

The sender is located... [Inside the organization](#)

add condition

\*Do the following...

Use the following connector... [ESG Outbound](#)

add action

Except if...

add exception

Properties of this rule:

☒ Audit this rule with severity level:

Not specified

Choose a mode for this rule:

Save Cancel

- Click on **add exception**.
- Except if -> the recipient -> is External/Internal -> inside the organization (this will not allow internal messages to be routed through Libraesva ESG)
- or -> the message properties -> include the message type -> automatic reply
- or The Sender -> IP address in any of these ranges or exactly matches -> Libraesva ESG

IP Address (to avoid loop transport problems)

Except if...

✕ The recipient is located... [Inside the organization](#)

or

✕ The message type is... [Automatic reply](#)

or

✕ Sender's IP address is in the range... [85.159.115.49/32](#)

add exception

- finally save the transport rule.

## Outbound Mail Flow

Now you have two **different scenarios** to deliver messages:

- 1) Deliver outgoing messages through Libraesva ESG IP Address (**MSP mode**)

✕**NOTE: This configuration is the one to be used if you are a MSP or if you manage multiple M365 tenants on one Libraesva ESG.**

In this scenario all outgoing email are delivered to the final destination by your Libraesva ESG directly, performing MX lookups and using it's own IP address. You have full control and responsibility of the node reputation.



If you opt for this scenario, the configuration finished, and you do not have to perform any other operation.

- 2) Deliver outgoing messages through Microsoft365 IP Address Space **(Recommended, not supported for MSP configurations)**

×**WARNING: This configuration is NOT supported if you are a MSP or if you manage multiple M365 tenants on one Libraesva ESG as it will cause tenant Attribution problems or loops on Microsoft.**

In this scenario all outgoing messages are routed back on to Microsoft 365 to be delivered to the final destination. The address space and reputation is managed by Microsoft - **Recommended setup for most cases.**



If you opt for this scenario you have to configure another 365 inbound connector and then add a smarthost to Libraesva ESG.

## Configure an Inbound Connector for the outbound mail flow

In the Exchange Admin Center, create another **Inbound Connector**, this connector will be use to receive the outbound mail coming back from ESG:

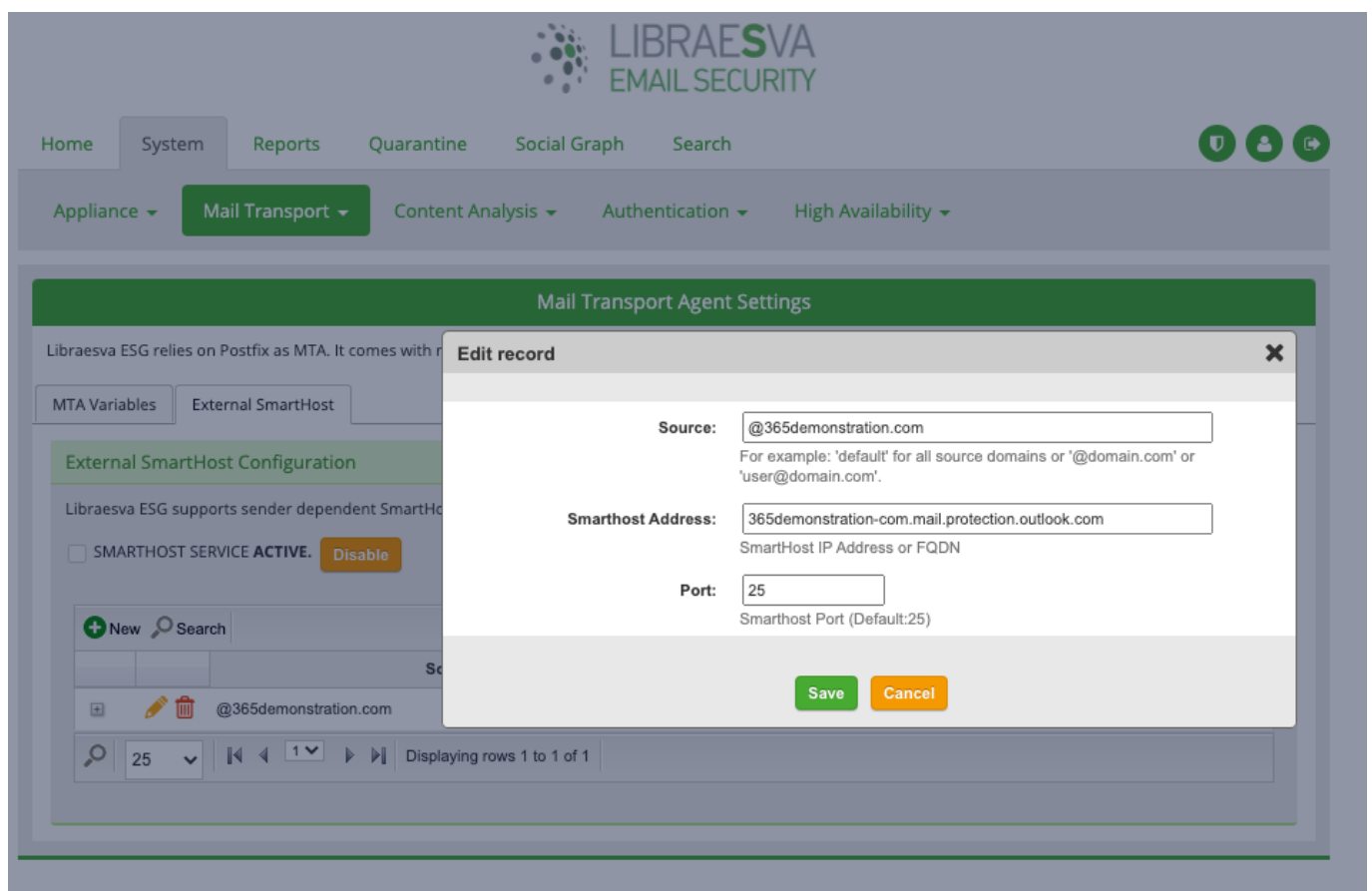
- 1) On the left side client **Mail Flow** and select **Connectors** on the top right
- 2) Under **Connectors**, click the [+] button.
- 3) From: **Your organization's mail server** - To: **Office 365**
- 4) Click **Next**.
- 5) Give it a name and click **Next**
- 6) Select **By verifying that the subject name on the certificate**
- 7) Specify the **hostname** of your Libraesva ESG appliance(s)
- 8) Click **Next**
- 9) Review and **Save**

×NOTE: Now you have to wait till 24h before enabling smarthost. Sometimes Microsoft takes a long to propagate settings. If you don't wait you might receive a M365 error saying Tenant Attribution Error.

Login to your Libraesva ESG appliance.



- Click Menu System->Mail Transport->MTA Advanced Configuration->External Smarthost
- Click **New**
- Enter as Source: @<your-domain>
- Smarthost Address: your 365 MX record (i.e. you-domain-com.mail.protection.outlook.com)
- Port: 25
- Click **Save**



## Import Users and Valid Recipients

Libraesva Email Security Gateway offers native integration with Microsoft Microsoft 365. In order to retrieve information such users, groups and email addresses from an Microsoft 365 tenant you can follow the instructions here:

<https://docs.libraesva.com/document/system/authentication/office-365-configuration/>

# Setup Threat Remediation

Libraesva ESG supports Email Threat Remediation, a feature to recall delivered messages from user's mailboxes. To setup this feature please follow this guide:

<https://docs.libraesva.com/document/threat-remediation/office-365-threat-remediation-settings/>